LAUR-03-4189

Paradigm Shifting Physical Security: From Keystone Kops to a Rigorous Discipline

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Los Alamos National Laboratory
Los Alamos, New Mexico

(505) 667-7414
rogerj@lanl.gov
http://pearl1.lanl.gov/seals

Definition

physical security: measures designed to protect important assets from physical harm.

The “assets” can include people, buildings, equipment, materials, documents, products, merchandise, food & drink, drugs, chemicals, weapons, money, and museum artifacts.

The “harm” that we wish to avoid includes theft, destruction, sabotage, vandalism, terrorism, espionage, forgery, tampering, or unauthorized access.

Existing Paradigms

Being a blockhead is sometimes the best security against being cheated by a man of wit.

-- Francois La Rochefoucauld, 1613-1680

Existing Paradigms (con't)

Keystone Kops, 1912-1917

Why Physical Security is So Difficult

- The traditional performance measure for security is pathological: success is defined as nothing happening.
- Cost/Benefit analyses is difficult.

- There are few meaningful standards, fundamental principles, models, or theories.
- Everything is a compromise & a tradeoff.

Why Physical Security is So Difficult (con't)

- Objectives are often remarkably vague.
- Adversaries and their resources are usually unknown to security managers, yet the adversaries understand the security systems.
- Effective security management is highly multi-disciplinary: technology, psychology, sociology, management, communication, law.
- Adversaries may be creative, non-linear thinkers. Security personnel often are not.

~

Why Physical Security is So Difficult (con't)

- Adversaries can attack at one point, but security managers may need to protect extended assets.
- Whereas adversaries need only identify and exploit one or a few vulnerabilities to succeed, security mangers must identify, prioritize, & manage many vulnerabilities, including unknown ones.
- Society does not always like security.

Why Physical Security is So Difficult (con't)

- Physical Security is not really a "field"

  - You can't get a degree in it.
  - Not widely attracting young people, females, the best and the brightest.
  - No peer-review, scholarly journals.* (The Journal of Physical Security)
  - Few conferences where R&D results are presented; Indeed, R&D and controlled experiments are frequently alien concepts.
  - Lots of snake oil salesmen.
  - Shortage of models, fundamental principles, metrics, rigor, critical thinking, & creativity.
  - Often dominated by bureaucrats, committees, "old boys" networks, linear/concrete/wishful thinkers.

The Journal of Physical Security

http://jps.lanl.gov

Other Security Problems

The insider threat is usually overlooked and/or difficult to deal with.

Disgruntled employees are a particular insider threat.

Disgruntlement by employees worldwide may be growing.

Americans are particularly susceptible to disgruntlement.

Disgruntled Workers

- Management research shows that employee disgruntlement is associated with perceptions of unfairness & inequity, not necessarily objective conditions.

- Disgruntled employees are known to be a risk for workplace violence, espionage, theft, and sabotage.

- Disgruntlement is probably increasing world-wide for general employees.

Causes of Increasing Worldwide Employee Disgruntlement

- global downsizing
- weakening of labor unions & collective bargaining
- increased use of temp & limited-term employees
- the disappearance of lifetime employment
- increased workforce diversity

Causes of Increasing Worldwide Employee Disgruntlement (con't)

- technical obsolescence
- the rapid pace of organizational change
- increased whistle-blowing
- depersonalization caused by increased urbanization, expanding government bureaucracy, the growth of multinational corporations, and the increased use of email & virtual meetings

Disgruntled Americans

American employees are particularly at risk for disgruntlement due to characteristic traits:

- identity is based on work
- work long hours
- strong individualism
- traditional belief in fairness
- traditional belief in “American Dream”

“Americans do not abide very quietly the evils of life.”

--historian Richard Hofstadter

Other Security Problems (con't)

- **Complaint resolution processes, which can help deal with disgruntled employees, are often non-existent, ineffective, adversarial, or fraudulent in high-security organizations.**

- **It's common to have overconfidence & believe the organization's press releases.**
- **It's common to confuse inventory & security functions, e.g., GPS.**
- **Problems with Vulnerability Assessments.**

Definition

vulnerability assessment: discovering and demonstrating security problems and flaws. Often also includes suggesting countermeasures.

Tricky Aspects of Vulnerability Assessments (VAs)

- Absolutist, binary ideas about security
- Misconception that vulnerabilities are bad news
- Misconception that security devices, systems, or programs should “pass” a VA
- “Shoot the Messenger” syndrome

Tricky Aspects of VAs (con't)

- Conflicts of interest
- No meaningful standards or underlying theory
- No clear endpoint
- Defeats are a matter of degree & probability

%

Tricky Aspects of VAs (con't)

- Recursion (chasing a moving target)
- Adversaries & their resources/capabilities are usually unknown.
- Most security failures are due to human error. (hard to model and predict)
- Experimental realism is difficult to achieve.

?

Better Paradigm?

- more education & professionalism
- emphasis on R&D (including psychological) and controlled experiments
- peer review
- realization that physical security is very challenging, not a sure thing
- realistic VAs & attitudes towards VAs

Better Paradigm? (con't)

- better cost/benefit analysis
- more sophisticated attitudes about security by officials and citizens
- stop looking for scapegoats
- more creativity & thinking outside the box (and tolerance for doing this)